UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/086,516	02/28/2002	Khanh V. Nguyen	50325-0644	2155

29989 7590 03/16/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/086,516	NGUYEN ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/03/2006 has been entered.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over J. Franks et al. herein after Franks "An Extension to HTTP : Digest Access Authentication" in view of Garrison Pub. No.: US 2001/0011349 A1.

Regarding claims 1, 24, 26, and 28, Franks teaches a method/medium/apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transfer protocol, the method comprising the computer-implemented steps of:

selecting a subset (*password/username*) of data for encryption from a set of data to be communicated between the client and the server in a particular payload (*a single message*

exchanged between client and server) of the unencrypted transfer protocol (section 1.2; *plurality of payloads/communications are exchanged between the client and server and a password or username is selected for encryption from a single payload and a password/username is never sent in clear*);

determining a secret integer (*common key*) that is unique (abstract, and section 2.1.1-2.1.2);

based on the subset (*password/username*) and the secret integer, generating encrypted data (*encrypted password/username*) that is impractical for a device other than the client and the server to decrypt (section 2.1.1, 2.1.2, and 2.1.3; *encrypted message.... password/username.... secrete common key*); and

sending, from a sending device of the client and the server to a receiving device of the client and the server, in the particular payload, the encrypted data and clue (*nonce, realm, domain,...)*

information to determine, only at the client and the server, the secret integer for decrypting the encrypted data (section 2.1.1, 2.1.2, and 2.1.3; *encrypted message and clue information in a payload...to determine decrypting key... is exchanged between client and server*).

Franks fails to explicitly disclose the applied secret integer is unique for the subset among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads;

However Garrison discloses the applied secret integer (*encryption key*) is unique for the subset among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload (*particular session*) is unique relative to secret integers associated with other payloads of the plurality of payloads (0012-0017, 0040, 0044, and claims 1 & 3; ***a new unique encryption key is generated for each single data payloads exchanged, in a session, between a server and client***);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Garrison's generating a unique encrypting key for each data payload in the session between a client and a user within the system of Franks because it would enhance security (0012 and 0009). ***One would have been motivated to do so because it would prevent hackers from discovering a valid password through a variety of hacking methods by intercepting data communications between the server and authorized client.***

Regarding claims 14, 25, 27, and 29, Franks teaches a method/apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload associated

with the transport protocol, the method comprising the computer-implemented steps of:

receiving, at a receiving device of the client and the server from a sending device of the client and the server, in a particular payload of the unencrypted transfer protocol, encrypted data and clue information (nonce, *realm, domain, ...)* to determine, only at the client and the

server, a unique secret integer (section 2.1.1, 2.1.2, and 2.1.3; *encrypted message and clue information in a payload...to determine a unique decrypting key... is received);*

determining the secret integer based, at least in part, on the clue information (section 2.1.1, 2.1.2, and 2.1.3; *based on the determined nonce, realm, domain... decryption key is determined and/or data is authenticated*); and

based on the secret integer, decrypting the encrypted data to generate a subset (*password/username*) of data communicated between client and server, wherein the subset (*password/username is never sent in clear*) is encrypted when transferred from the sending, device to the receiving device (section 2.1.1, 2.1.2, and 2.1.3; *based on the determined nonce, realm, domain... decryption key is determined/decrypted and/or data is authenticated*).

Franks fails to explicitly disclose the applied secrete integer being unique for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads.

However Garrison discloses a unique secrete integer (*encryption key*) for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload (*particular session*) is unique relative to secret integers associated with other payloads of the plurality of payloads (0012-0017, 0040, 0044, and claims 1 & 3; ***a new unique encryption key is generated for each single data payloads exchanged, in a session, between a server and client***);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Garrison's generating a unique encrypting key

for each data payload in the session between a client and a user within the system of Franks because it would enhance security (0012 and 0009). ***One would have been motivated to do so because it would prevent hackers from discovering a valid password through a variety of hacking methods by intercepting data communications between the server and authorized client.***

Regarding claims 2 and 15, Franks further teaches a method, wherein the unencrypted transfer protocol is Hypertext Transfer Protocol (HTTP) (section 2.1).

Regarding claim 3, Franks further teaches a method, said step of determining a secret integer that is unique for the subset further comprising the steps of:

generating a first integer using a random number generator (section 2.1.1);

determining a shared secret key to be shared with the receiving device based on the first integer and a first public key associated with the receiving device (section 2.1.1); and

selecting the secret integer based on the shared secret key (section 2.1.1).

Regarding claim 4, Franks further teaches a method, said step of sending the information to determine the secret integer further comprising the steps of

determining a second public key associated with the sending device based on the first integer (section 2.1.1-2.1.2); and

including the second public key in the information to determine the secret integer (section 2.1.1-2.1.2).

Regarding claim 5, Franks teaches a method, said step of sending the information to determine the secret integer further comprising the steps of:

determining a plurality of second public keys associated with the sending device based on the first integer, wherein each of the second public keys is associated with one of a plurality of subsets from the set of data (section 2.1.1-2.1.2); and

including the plurality of second public keys in the information to determine the secret integer (section 2.1.1-2.1.2).

Regarding claim 6, Franks further discloses a method, said step of setting the secret integer further comprising the step of applying a particular hash function to the shared secret key to generate the secret integer (section 2.1.1).

Regarding claim 7, Franks further teaches a method, said step of generating encrypted data further comprising the step of performing an exclusive or (XOR) operation between corresponding bits of the subset and the secret integer to generate the encrypted data (section 2.1.1; *concatenating data with secrete*).

Regarding claim 8, Franks further teaches a method as recited, wherein:

said step of determining the secret integer further comprises the step of applying a particular hash function a plurality of times to a shared secret key shared with the receiving device (section 2.1.1); and

said step of sending the information to determine the secret integer further comprises the step of storing, as part of the clue information, data that indicates a number of times the particular hash function has been applied (section 2.1.1; *data string is uniquely generated/hashed each time response/payload is made*).

Regarding claims 9 and 20, Franks further teaches a method, said step of determining the secret integer
further comprising the steps of:

determining a first integer formed after the particular hash function is applied the number of times indicated in the information (section 2.1.1);

determining a second integer formed after the particular hash function is applied fewer times than the number of times indicated in the information (section 2.1.1-2.1.2); and

performing an exclusive or (XOR) operation between corresponding bits of the first integer and the second integer (section 2.1.1).

Regarding claims 10 and 21, Franks further teaches a method, said step of determining the secret integer
further comprising the steps of

determining a first integer formed after the particular hash function is applied the number of times indicated in the information (section 2.1.1);

determining a second integer formed after a second hash function is applied for the number of times indicated in the information, wherein the second hash function is different

from the particular hash function that is used to determine the first integer (section 2.1.1-2.1.2); and

performing an exclusive or (XOR) operation between corresponding bits of the first integer and the second integer (section 2.1.1).

Regarding claim 11, Franks further teaches a method, further comprising, before said step of determining the secret integer, performing the steps of

determining the shared secret key based on a particular communication between the client and the server (abstract, and section 2.1.1-2.1.2); and

storing the shared secret key in a secure data structure (abstract, and section 2.1.1-2.1.2).

Regarding claims 12 and 13, Franks further teaches a method, wherein the secret integer has a particular number of bits fixed for all subsets in all payloads communicated during a communication session between the client and the server (abstract and page 5 par. 1-7).

Regarding claim 13, Franks further teaches a method, wherein the secret integer has a number of bits that varies in accordance with lengths of payloads that are communicated during a communication session between the client and the server (page 5 par. 1-7).

Regarding claim 16, Frank further teaches a method, said step of determining the secret integer further comprising the steps of:

based on the clue information, determining a shared secret key shared with the

sending device (section 2.1.1, 2.1.2, and 2.1.3; *based on the determined nonce, realm, domain... decryption key is determined/decrypted and/or data is authenticated*); and

generating the secret integer based on the shared secret key (section 2.1.1-2.1.2).

Regarding claim 17, Franks further teaches a method, said step of generating the secret integer further comprising the step of applying a particular hash function to the shared secret key to generate the secret integer (page 5 lines 10).

Regarding claim 18, Franks further teaches a method, wherein:
the method further comprises the steps of

determining a shared secret key based on a particular communication between the client and the server (section 2.1.1-2.1.1), and

storing the shared secret key in a secure data structure; and
the clue information indicates a number of times a particular hash function is applied to the shared secret key in generating the secret integer (section 2.1.1-2.1.1).

Regarding claim 19, Franks further teaches a method, said step of determining the secret integer further comprising the step of causing the particular hash function to be applied the number of times indicated by the clue information to the shared secret key (section 3.2 and 2.1.1)

Regarding claim 22, Franks further teaches a method, said step of decrypting the encrypted data further comprising the step of performing an exclusive or (XOR) operation between

corresponding bits of the encrypted data and the secret integer to generate the subset of data (section 2.1.1).

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.
March 10, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100